Information and Privacy
Commissioner/Ontario
Commissaire à l'information
et à la protection de la vie privée/Ontario

GUIDELINES ON FACSIMILE TRANSMISSION SECURITY

EXECUTIVE SUMMARY

The facsimile (commonly referred to as "fax") is a widely used method of communicating information from one location to another. Recent incidents have occurred where documents were inadvertently transmitted to the wrong destination. Such situations not only raise the issue of compromised confidentiality, but also have implications for the *Freedom of Information and Protection of Privacy Act, 1987* (the "*Act*"). One of the purposes of the *Act* is to protect the privacy of individuals with respect to personal information about themselves held by government institutions. The Commissioner's office thought it was important at this time to develop proposed guidelines relating to fax security transmission, in order to preserve the confidentiality of information transmitted by fax.

A number of security features are available on fax machines such as key locks, confidential mail boxes, and encryption features, however most fax machines currently in use do not include these features.

The physical location of a fax machine has a significant impact on the security implications of fax transmissions. Offices often locate their fax in a relatively public place where it can be used by virtually anyone. This enables uncontrolled access to incoming fax information and creates potential problems in maintaining confidentiality of personal information. Also, the sender is usually unaware of the receiver's operating environment, thereby adding an additional level of concern.

... Guidelines on next page ...

80 Bloor Street West,
Suite 1700,
Toronto, Ontario
M5S 2V1

Fax: 416-965-2983
1-800-387-0073
Tel: 416-326-3333

SUMMARY OF GUIDELINES

Personal information and exempt records (as defined in the *Act*) should not be transmitted by fax:

If there is an urgent need to transmit this information by fax, all personal identifiers should be removed from the documents, thereby removing the information from the definition of "personal information" as defined under the *Act*.

The fax machine should only be used by authorized persons:

By restricting the use of the fax machine to authorized persons, the potential for unauthorized disclosure is reduced should another office inadvertently fax confidential information.

The Fax machine should be located such that:

- it is not in a public area;
- its use can be monitored by the responsible person;
- only authorized staff can have access to information transmitted on the fax.

Procedures should be implemented to ensure that information is sent to the intended fax number:

Unlike erroneously addressed mail which may be returned unopened, documents faxed to the wrong number can be read by a number of people. In order to avoid this situation, institutions should take appropriate precautions to ensure that documents are directed to the correct fax number. The destination fax number should always be reconfirmed **prior to transmission**.

Information should be transmitted completely and securely:

The sender should confirm the success of the fax transmission by checking the Fax Activity Confirmation Report.

Information should reach the intended recipient:

Although information may be sent to the correct fax number, it could, nonetheless, reach the wrong recipient. The first page of all faxed documents should be a fax cover sheet, identifying the sender and the intended recipient.

Information should be received completely:

The receiver should check the number of pages actually received against the transmitted Fax cover sheet.

Information and Privacy
Commissioner/Ontario
Commissaire à l'information
et à la protection de la vie privée/Ontario

Guidelines

on

Facsimile Transmission Security

June 1989

80 Bloor Street West,
Suite 1700,
Toronto, Ontario
M5S 2V1

Fax: 416 965-2983
1-800-387-0073
Tel: 416 326-3333

89-06393/

TABLE OF CONTENTS

		Page
1.	INTRODUCTION	1
2.	BACKGROUND DISCUSSION	2
3.	GUIDELINES	6

1. INTRODUCTION

1.1 Background

The facsimile (commonly referred to as "fax") is a widely used method of communicating information from one location to another. Essentially, the fax machine has the ability to send and receive copies of documents over ordinary telephone lines. In a typical fax transaction, the document to be faxed is placed in the document feeder of the fax unit; then the telephone number of the fax unit to which the document is to be sent is dialed. In a short time, a replica of the original document is printed out at the destination fax unit.

Situations have already occurred where documents have been inadvertently transmitted to the wrong destination. This can happen if the sender dials the wrong destination fax number, or if the intended recipient is not available to accept the faxed document and another person takes custody of it. Such situations not only raise the issue of compromised confidentiality, but also have implications for the *Freedom of Information and Protection of Privacy Act, 1987* (the *Act*). One of the purposes of the *Act* is to protect the privacy of individuals with respect to personal information about themselves held by government institutions. In the absence of specific directives, it is possible that government institutions may be using the fax to transmit sensitive, personal information. We are, in fact, aware of this very occurrence.

Recognizing these risks, the Office of the Information and Privacy Commissioner/ Ontario (IPC) has prepared a set of proposed guidelines for government institutions to consider when using the fax.

1.2 Objectives of this document

The purpose of this document is to set out guidelines for government institutions to consider when developing systems and procedures to maintain the confidentiality of information being transmitted by fax.

1.3 Approach

All organizations should have control over various activities that are performed within their organization. How they exercise this control varies from one organization to another. The objective is to ensure that desired events do take place (i.e. only authorized persons obtain access to sensitive information), and undesirable events do not take place (i.e. breaches of security). Clearly defined objectives enable an organization to achieve the desired level of control over its activities.

Specific control objectives necessary to maintain the confidentiality of information being transmitted have been explored. Attributes considered necessary to achieve these objectives are then identified.

1.4 Future Developments

While the security features associated with fax machines are relatively limited at the present time, the industry is in a state of flux, and significant developments in this area may be anticipated over the next year. The present guidelines will be updated in one year's time (or possibly earlier, if the need arises), to reflect any changes associated with new security features.

A recent development, that will undoubtedly increase in the absence of legislation, is what is popularly known as "junk fax". Organizations are using the fax to transmit unsolicited advertisements and press releases. This activity not only results in unwanted documents being received, but ties up the receiver's fax machine and uses up the receiver's stationary. In mid-May 1989 the State of Connecticut barred unsolicited advertising messages from being sent to fax machines in the state. Several other U.S. states are also in the process of considering similar legislation.

2. BACKGROUND DISCUSSION

2.1 Types of Information

All information held by government institutions does not require the same degree of security when communicated from one source to another. Thus, the first stage in the development of these guidelines was to categorize the various types of information held by government institutions.

The Government of Canada, in Part I section 3.1 of its Interim Security Standards: Operating Directives and Guidelines, categorizes information into:

- classified in the national interest; and
- protected but not in the national interest.

Unlike the federal government, the concept of "classified" or highly protected information does not exist within the Ontario government. Thus, for the purposes of these guidelines, the IPC used the requirements of the *Act* as the basis for categorizing information held by government institutions.

Under the *Freedom of Information and Protection of Privacy Act,1987*, records in the custody or control of a government institution in Ontario may be categorized as:

- Personal Information (Section 2 of the *Act*);
- Exempt Records (if they fall under Sections 12 through 22 of the *Act*);
- General Records (information other than Personal Information and Exempt Records as defined above).

Part III of the *Act*, which deals with the protection of individual privacy, requires that personal information held by institutions be protected from unauthorized use or disclosure, and regulates the collection, use, disclosure and disposal of personal information.

The *Act* also provides a right of access to a record or part of a record in the custody or control of a government institution, unless it falls within one of the exemptions contained in sections 12 through 22. Thus, exempt information should also be protected from unauthorized use or disclosure.

2.2 Existing Technology

At present, fax machines transmit and receive copies of documents over ordinary telephone lines. Therefore, like a telephone conversation, fax transmissions can be tapped and intercepted by unauthorized third parties. One method of avoiding this problem is for information to be encrypted or encoded so that it is rendered meaningless and cannot be read directly. The Government of Canada in Part III, Section B, Subsection 2.11.1, Interim Security Standards: Operating Directives and Guidelines, requires that classified information and other sensitive information designated as PROTECTED shall not be communicated in record communication systems, such as facsimile, unless the information has been cryptographically protected.

One of the manufacturers contacted by the IPC markets a fax with an encryption feature. This fax unit, however, can only transmit encrypted information between identical fax units. This consideration would thus appear to be far from practical at the present time for ordinary users.

Encrypted information may also be transmitted between computers and decrypted or decoded at the receiving computer. A fax attached to the destination computer could be used to print the transmitted information. A practical problem in using this procedure is that all the information required to be faxed may not be held on computers. For example, text such as minutes of meetings and other hand-written notes, may not be

stored on a computer. For such information to be faxed securely, it must first be transferred to a computer. Such a procedure is neither practical nor cost effective for ordinary users.

Therefore, under existing commercially available fax technology, encryption does not appear to be a satisfactory solution in most situations, but its use should be considered when sensitive information is involved.

2.3 Existing Capabilities of Fax Machines

Existing commercially-available fax technology and the scarcity of fax machines with a variety of security features have created limitations in achieving secure facsimile transmission.

Fax units are generally capable of printing a history of fax activity based on either a time span or volume of activity. For example, the fax unit can be set to automatically print a history of its activity after every 40 transactions.

This Fax Activity History Report is helpful in monitoring the use of the fax and to account for its activity. On most fax machines, however, once this report has been printed, it cannot be reprinted. As a result, it is possible for an unauthorized user to print these activity reports and destroy them, leaving no trace of unauthorized activity. A person could thus remove an incoming faxed document not intended for him, and eliminate any trace of the transaction by printing and destroying the activity report. Features do exist, however, on some fax machines which provide certain controls to overcome these problems.

i) Keylocks

The fax machine can be locked with a key. Unless it is unlocked, information cannot be transmitted nor can incoming information be printed. Thus, by installing a keylock, virtually all categories of information are subject to the same degree of security. This security procedure may not be practical where the fax has been acquired for general office use. There is also a risk that incoming information waiting to be printed can be lost in the case of a power loss to the fax. Manufacturers can provide an optional battery backup if required. In order to preserve information, certain models also store information on a data disk.

ii) Confidential Mailboxes

Certain fax units enable a document to be transmitted so that it can be received only by a specific person. This feature is commonly referred to as a "private or confidential mailbox". It is a memory location within the fax unit that stores incoming documents.

Practically, the number of confidential mailboxes in a fax unit is limited. The sender's fax unit must also be able to transmit to a fax unit with the same mailbox feature.

Documents can be transmitted to the intended receiver's confidential mailbox and printed out after a correct password is entered. This password is user-selected and can be changed by either supplying the old password or by using a master password held by the manufacturer. On most fax machines passwords are protected from loss due to temporary power lapses. However, the master password held by the manufacturer is usually the same for all of its products. Thus, it is possible for this master password to be widely known, thereby compromising security. In order to ensure confidentiality, the receiver would have to print the document immediately after it is received by the fax unit.

iii) Activity Confirmation Reports

Almost all fax machines print a confirmation of activity each time they are used. These reports confirm whether the transmission has been successful, and print the destination fax number and the number of pages transmitted. Thus, the sender can use it as some form of assurance that the documents have been transmitted correctly. The receiver can use the report to ensure that all transmitted pages have been received.

2.4 User Environment

The physical environment in which a fax is used may have a considerable impact on the security implications of fax transmissions. Offices sometimes situate their fax in a relatively public place where it can be used by virtually anyone, thus enabling unauthorized personnel to read incoming information. Such an environment makes it more difficult to maintain the confidentiality of personal information.

Another problem is that senders are usually completely unaware of the receiver's operating environment. The sender could fax confidential information on the presumption that the receiver's office procedures are secure, when in fact, they are not. Thus, non-standardized office procedures relating to fax use can result in the loss of confidentiality.

3. GUIDELINES

3.1 Personal Information and Exempt Records

Given the limitations of existing commercially-available fax technology, it is doubtful that the level of privacy protection required by the *Act* will be achieved. It is therefore recommended that personal information and exempt records, as defined in the *Act*, should **not** be transmitted by fax.

In emergency situations, where the recipient insists upon using fax as the mode of communication, the sender should send the information only to a confidential mailbox. This requirement is essential when transmitting highly sensitive, personal information. If a confidential mailbox is not available, personal information and exempt records should never be faxed.

However, if personal identifiers are removed from the document to be transmitted, then the document would no longer be considered "personal information", as defined by the *Act* . The removal of personal identifiers takes the information outside of the scope of "any information about an **identifiable** individual" and would thus enable the document to be faxed. Alternatively, the severance of personal information would also permit the faxing of documents of this nature.

3.2 General Records

i) **The fax machine should only be used by authorized persons.**

Persons authorized to use the fax would normally consist of office support staff. In a small to medium sized office, individual staff members may personally transmit documents. In a larger office, with a high volume of fax transmissions, consideration should be given to centralizing fax operations. By restricting use of the fax to authorized persons, the potential for unauthorized disclosure is reduced, should another office inadvertently fax confidential information.

- One person (and a backup) should be identified as responsible for all fax operations. Therefore, in case of problems, technical or otherwise, staff know who to contact.

- The fax machine should be located such that:

    - it is not in a public area;

    - its use can be monitored by the responsible person;

    - only authorized staff have access to information transmitted on the fax.

- Certain institutions may have to use the fax to communicate information requiring extra security protection. In these cases, the fax should be equipped with a keylock dedicated to this purpose.

- Fax machines should not be shared by institutions. Sharing results in the need to allocate or share confidential mailboxes, making it more difficult to maintain secure procedures.

ii) **Procedures should be implemented to ensure that information is sent to the intended fax number.**

Unlike erroneously addressed mail which may be returned unopened, a document faxed to the wrong number can be read by a number of people. In order to avoid this situation, institutions should take appropriate precautions to ensure that documents are directed to the correct fax number.

- A master list of authorized fax numbers should be maintained to serve as a reference list.

- The destination fax number should be reconfirmed before transmission. Unlike most ordinary telephones, the number being dialed from a fax unit is displayed on a screen similar to that on an electronic calculator. In existing fax machines, the destination fax number can be confirmed by physically checking the number displayed on the screen before transmitting the document.

- All fax machines used by government institutions should be able to print Fax Activity Confirmation Reports and Fax Activity History Reports.

- The sender should check the Fax Activity Confirmation Report for the accuracy of the destination fax number. This report should be retained with the original of the faxed document. Retaining the Fax Activity Confirmation Report provides a record that the document was faxed to the intended fax number.

- In case the document has been transmitted to the wrong fax number, the sender should immediately contact this organization, inform them of the error, and ensure that the faxed document is destroyed.

iii) Information should be transmitted completely and securely.

- The sender should confirm the success of the transmission by checking the Fax Activity Confirmation Report.

- All fax machines used by government institutions should be equipped with confidential mailboxes. Where confidentiality is required, information should be transmitted to a confidential mailbox. Government institutions should ascertain whether certain general records require extra protection because of their sensitivity.

iv) Information should reach the intended recipient.

Although information may be sent to the correct fax number, it could, nonetheless, reach the wrong recipient.

- The first page of all faxed documents should be a Fax Cover Sheet. It should identify the sender and the intended receiver. This page should eliminate any doubt regarding the intended receiver.

- The fax machine should be located so that only authorized persons can retrieve a document. (Refer to 3.2(1).)

- The receiver should initial the Fax Activity Confirmation Report. These reports should be in the custody of the person responsible for fax operations. (Refer to 3.2(1).)

- The person responsible for fax operations should review the Fax Activity Confirmation Reports (confirming receipt of a faxed document) to ensure that documents have been collected by the appropriate persons.

- In cases where a document has been transmitted to the wrong fax number, the recipient should inform the sender of the error, destroy the faxed document and note this action on the Fax Activity Confirmation Report. In cases where a document has been addressed to the wrong recipient, the actual recipient should re-direct the faxed document and make a corresponding notation on the Fax Activity Confirmation Report.

v) **Information should be received completely.**

- The receiver should check the number of pages actually received against the transmitted Fax Cover Sheet or against the Fax Activity Confirmation Report (in cases where no Fax Cover Sheet has been transmitted). If pages are missing, the sender should be contacted and asked to re-transmit the document.

- Consideration should be given to providing the fax with a battery backup in case of a power disruption. Institutions should consult their fax vendor.

- The fax machine should record on each page received:

  - the date and time received,
  - the fax number of the originator,
  - the name and identification of the originator, and
  - the page number of the document.

Sidney B. Linden
Commissioner

Ann Cavoukian, Ph.D.
Director of Compliance

Information and Privacy
Commissioner/Ontario
Commissaire à l'information
et à la protection de la vie privée/Ontario

DIRECTIVES CONCERNANT LA SÉCURITÉ DE TRANSMISSION PAR TÉLÉCOPIEUR

SOMMAIRE

Le recours au télécopieur est un moyen très répandu de communication de renseignements d'un point à l'autre. Récemment, il est arrivé qu'on transmette certains documents par erreur au mauvais destinataire. De telles situations concernent non seulement la question de confidentialité compromise, mais aussi la *Loi de 1987 sur l'accès à l'information et la protection de la vie privée* (la "*loi*"). L'un des objets de la *loi* est précisément de protéger la vie privée des particuliers de qui les institutions gouvernementales détiennent des renseignements personnels les concernant. C'est pourquoi le bureau du Commissaire a jugé que le moment était venu d'élaborer des directives sur la transmission sécuritaire des documents télécopiés, de manière à assurer le caractère confidentiel des renseignements ainsi transmis.

Il existe actuellement différents dispositifs de sécurité pour les télécopieurs, tels que des verrous de sécurité, des boîtes à lettres confidentielles et des dispositifs de chiffrement, caractéristiques que peu de télécopieurs actuels possèdent.

L'emplacement physique des télécopieurs est un facteur important de la transmission sécuritaire des documents par ce moyen. Dans la plupart des bureaux, le télécopieur est placé dans un endroit relativement public, à la portée de pratiquement n'importe qui. Ceci donne un accès non contrôlé aux informations d'arrivée et peut créer des problèmes de protection de renseignements confidentiels et personnels. Et comme le transmetteur est rarement au courant de la manière dont les documents d'arrivée sont traités, cela représente un problème de plus.

... Directives (suite) ...

80 Bloor Street West,
Suite 1700,
Toronto, Ontario
M5S 2V1

Fax 416 965-2983
1-800-387-0073
Tel 416 326-3333

SOMMAIRE DES DIRECTIVES

La communication de renseignements personnels et de documents faisant l'objet d'une exception (selon la définition de la *loi*) ne devrait pas se faire par télécopieur:

S'il y a un besoin urgent de transmettre des renseignements par télécopieur, toute désignation personnelle doit être éliminée des documents, de manière que le renseignement transmis ne constitue pas un "renseignement personnel" selon la définition de la *loi*.

Le télécopieur ne devrait être utilisé que par des personnes autorisées:

En limitant l'utilisation des télécopieurs aux personnes autorisées, cela réduit les risques de divulgation sans autorisation, lorsqu'un bureau transmet des renseignements de nature confidentielle par inadvertance.

Le télécopieur devrait être placé:

- ailleurs que dans un lieu public;
- de façon que son utilisation soit supervisée par la personne en charge;
- de façon que seul le personnel autorisé ait accès aux renseignements transmis par télécopieur.

Il faudrait mettre en place des procédures pour assurer la transmission de renseignements au numéro du télécopieur voulu:

Contrairement aux lettres mal adressées qui reviennent à l'expéditeur non décachetées, les documents télécopiés au mauvais numéro peuvent être lus par un certain nombre de personnes. Pour éviter une situation de ce genre, les institutions doivent prendre toutes les précautions nécessaires pour que les documents soient transmis au numéro de télécopieur correct. Le numéro du télécopieur récepteur devrait toujours être reconfirmé avant la transmission.

Les renseignements doivent être transmis au complet et en toute sécurité:

L'envoyeur doit s'assurer de l'envoi correct de sa transmission en vérifiant le rapport de confirmation des mouvements du télécopieur.

Les renseignements doivent parvenir à la personne à qui ils sont destinés:

Même si on envoie un document au numéro de télécopieur correct, il se peut qu'il parvienne au mauvais destinataire. La première page de tout document télécopié doit être une feuille d'accompagnement, identifiant l'expéditeur et le destinataire du document.

Les renseignements doivent être reçus au complet:

Le destinataire doit vérifier le nombre de pages effectivement reçues et le comparer au nombre de pages indiqué sur la feuille d'accompagnement transmise.

Information and Privacy
Commissioner/Ontario
Commissaire à l'information
et à la protection de la vie privée/Ontario

Directives concernant la sécurité de transmission par telecopieur

juin 1989

80 Bloor Street West,
Suite 1700,
Toronto, Ontario
M5S 2V1

Fax: 416 965-2983
1-800-387-0073
Tel: 416 326-3333

TABLE OF MATIÈRES

		Page
1.	INTRODUCTION	1
2.	ÉTABLISSEMENT DES FAITS	2
3.	DIRECTIVES	6

1. INTRODUCTION

1.1 Établissement des faits

Le télécopieur est un moyen très répandu de communication de renseignements d'un point à un autre. Le télécopieur a la capacité d'envoyer et de recevoir des copies de document par lignes téléphoniques ordinaires. Le document à communiquer est placé dans un dispositif d'alimentation du télécopieur, puis on compose le numéro de téléphone du télécopieur auquel on envoie le document. En peu de temps, une copie du document original sort du télécopieur destinataire.

Il est déjà arrivé que des documents soient transmis par erreur au mauvais destinataire. Cela se produit lorsque l'émetteur se trompe en composant le numéro du télécopieur récepteur, ou lorsque le destinataire du document télécopié n'est pas là pour le recevoir et qu'une autre personne le reçoit à sa place. De telles situations concernent non seulement la question de la mise en danger de la confidentialité, mais aussi la *Loi de 1987 sur l'accès à l'information et la protection de la vie privée* (la "*loi*"). L'un des objets de la loi est précisément de protéger la vie privée des particuliers concernés par des renseignements que détiennent les institutions gouvernementales. À défaut de directives précises, les institutions gouvernementales pourraient se servir d'un télécopieur pour transmettre des renseignements personnels, de nature délicate. C'est une possibilité dont nous sommes très conscients.

Pour éviter ce risque, le Bureau du commissaire à l'information et à la protection de la vie privée/Ontario propose un ensemble de directives pour les institutions gouvernementales qui se servent de télécopieurs.

1.2 Objets de ce document

Ce document a pour objet de proposer aux institutions gouvernementales des directives aptes à les guider au moment d'élaborer des systèmes et des procédures visant à maintenir le caractère confidentiel des documents transmis par télécopieur.

1.3 Méthode

Tout organisme doit avoir un certain contrôle des diverses activités qui y prennent place. L'exercice de ce contrôle varie d'un organisme à l'autre. Il doit assurer l'exécution correcte des tâches d'une certaine façon (par exemple, seules les personnes autorisées peuvent accéder aux renseignements de nature délicate) pour empêcher des incidents regrettables (comme la violation du caractère confidentiel d'un document). Des objectifs clairement définis permettent à un organisme d'exercer le niveau de contrôle souhaité sur ses activités.

Nous avons recherché des objectifs de contrôle précis pour maintenir le caractère confidentiel des renseignements transmis, et identifié les attributs jugés nécessaires à la réalisation de ces objectifs.

1.4 Progrès technologiques

Alors que les caractéristiques de sécurité associées aux télécopieurs d'aujourd'hui sont relativement limitées, on peut s'attendre à de grands progrès technologiques dans ce domaine d'ici quelques années. Ces directives seront donc mises à jour dans un an (ou même plus tôt), en fonction des changements au niveau des dispositifs de sécurité.

Un récent phénomène, susceptible d'empirer en l'absence d'une loi à cet égard, est celui de la transmission de documents importuns, par des organismes qui se servent d'un télécopieur pour transmettre de la publicité et des communiqués de presse non sollicités. Cette activité donne lieu, non seulement à une avalanche de documents indésirables, mais encombre le télécopieur-récepteur dont elle gaspille le papier. En mai 1989, le Connecticut a interdit la transmission télécopiée de messages publicitaires non sollicités dans son État. D'autres États américains étudient la possibilité d'imposer une loi analogue.

2. ÉTABLISSEMENT DES FAITS

2.1 Types de renseignements

Tout renseignement détenu par une institution gouvernementale ne demande pas le même degré de protection lorsque transmis d'une source à l'autre. C'est pourquoi nous avons commencé par classifier les différents types de renseignements en possession des organismes gouvernementaux.

Le gouvernement du Canada (Partie I, article 3.1 de ses Normes provisoires de sécurité: Directives et lignes directrices d'utilisation) classifie les renseignements en:

- classifiés dans l'intérêt national; et
- protégés, en tant qu'autres renseignements.

Contrairement au gouvernement fédéral, le concept d'un renseignement "classifié" ou hautement protégé n'existe pas au sein du gouvernement de l'Ontario. Le commissaire à l'information et à la protection de la vie privée s'est donc inspiré de la *loi* pour classifier les renseignements détenus par les institutions gouvernementales.

Aux termes de *la Loi de 1987 sur l'accès à l'information et la protection de la vie privée*, les documents dont une institution a la garde ou le contrôle en Ontario peuvent être classifiés en tant que :

- renseignements personnels (section 2 de la *loi*);

- documents faisant l'objet d'une exception (si ces cas relèvent des articles 12 à 22 de la *loi*);

- documents généraux (documents autres que les renseignements personnels et documents d'exception définis ci-dessus).

La partie III de la *loi*, qui traite de la protection de la vie privée, exige que les renseignements personnels détenus par les institutions soient protégés de toute utilisation ou divulgation non autorisée, et réglemente la collecte, l'utilisation, la divulgation et la disposition de renseignements personnels.

La *loi* autorise l'accès à un document ou à une partie d'un document dont une institution gouvernementale a la garde ou le contrôle, à moins que ledit document ne fasse partie des exceptions visées aux articles 12 à 22. Ainsi, les documents faisant l'objet d'une exception doivent aussi être protégés de toute utilisation ou divulgation non autorisée.

2.2 Technologie d'aujourd'hui

Nos télécopieurs actuels transmettent et reçoivent des copies de documents sur une ligne téléphonique ordinaire. Donc, tout comme une conversation téléphonique, une transmission par télécopieur peut être branchée et interceptée par des tiers non autorisés. Une manière d'éviter ce problème consiste à chiffrer ou coder les renseignements, de manière à les rendre incompréhensibles à la lecture directe . Dans la Partie III, article B, paragraphe 2.11.1 de ses Normes provisoires de sécurité : Directives et lignes directrices d'utilisation, le gouvernement du Canada demande que les renseignements classifiés et ceux de nature délicate désignés comme protégés ne soient pas transmis au moyen de systèmes de communications, comme les télécopieurs, à moins de protéger cryptographiquement ces renseignements.

Un des fabricants contactés par le commissaire à l'information et à la protection de la vie privée vend un télécopieur avec dispositif de chiffrement. Mais comme ce télécopieur ne peut transmettre de renseignements codés qu'entre télécopieurs identiques, cela ne présente pas beaucoup d'intérêt pour les usagers courants d'aujourd'hui.

On peut également transmettre des renseignements codés d'un ordinateur à l'autre, à déchiffrer et décoder par l'ordinateur récepteur. Un télécopieur branché sur l'ordinateur destinataire pourrait servir à imprimer les renseignements transmis. Ce procédé

présente un problème en ce sens que les renseignements à télécopier ne peuvent pas être gardés sur ordinateur. Par exemple, des textes comme des procès-verbaux de réunions et autres notes écrites à la main ne peuvent pas être conservés dans l'ordinateur. Pour télécopier de tels renseignements d'une manière sécuritaire, il faudrait d'abord les transférer sur ordinateur. Un tel procédé n'est ni pratique ni rentable pour les utilisateurs courants.

Donc, dans le cadre de la technologie de télécopieur actuelle, le chiffrement ne semble pas convenir dans la plupart des cas, mais il pourrait peut-être servir à transmettre des renseignements de nature délicate.

2.3 Capacité actuelle des télécopieurs

La technologie actuelle des télécopieurs d'usage courant et le nombre restreint de télécopieurs équipés de dispositifs de sécurité imposent certaines limites à la transmission sécuritaire des copies.

Les télécopieurs sont généralement capables de produire un rapport "historique" de leurs mouvements, exprimés en temps ou en volume d'activité. Par exemple, on peut régler un télécopieur de manière qu'il imprime automatiquement la liste de ses activités après 40 opérations.

Le rapport "historique" des mouvements du télécopieur est une bonne façon de contrôler l'utilisation et l'activité de la machine. Cependant, comme la plupart des télécopieurs ne peuvent réimprimer un rapport déjà imprimé, un utilisateur non autorisé peut très bien imprimer ces rapports de mouvements et les détruire, effaçant ainsi toute trace d'activité irrégulière. Une personne pourrait ainsi enlever un document transmis par télécopieur qui ne lui est pas adressé, et éliminer toute trace de la transaction en imprimant puis en détruisant le rapport des mouvements. Cependant, certains télécopieurs sont équipés de dispositifs permettant d'éliminer jusqu'à un certain point ces problèmes.

i) Verrous de sécurité

On peut verrouiller un télécopieur à l'aide d'une clé. Il est impossible de transmettre ou de recevoir des documents avec un télécopieur verrouillé. Donc, en installant un verrou, on donne à presque toutes les catégories de renseignements le même degré de protection. Cette mesure de sécurité peut ne pas convenir à un télécopieur à utiliser par tout le bureau. On court aussi le risque de perdre les renseignements d'arrivée à imprimer, advenant une panne. Le fabricant peut fournir, sur demande, une batterie de secours facultative. Pour conserver les renseignements, il existe des modèles qui stockent les renseignements sur disques de données.

ii) **Boîtes à lettres confidentielles**

Certains télécopieurs transmettent un document qui ne peut être reçu que par la personne désignée, grâce à un dispositif qu'on désigne généralement par "boîte à lettres privée ou confidentielle". C'est l'adresse de mémoire à l'intérieur du télécopieur qui stocke les documents d'arrivée.

Dans la pratique, le nombre de boîtes à lettres confidentielles d'un télécopieur est limité. Il faut aussi que le télécopieur émetteur puisse transmettre à un télécopieur ayant le même dispositif "boîte à lettres".

On peut transmettre et imprimer des documents à la boîte à lettres confidentielle du destinataire voulu après avoir entré le mot de passe correct. On peut changer ce mot de passe, choisi par l'utilisateur, soit en fournissant l'ancien mot de passe, soit en se servant du mot de passe maître du fabricant. La plupart des télécopieurs sont équipés d'un dispositif qui empêche le mot de passe de se perdre en cas de panne. Mais comme le mot de passe maître du fabricant est généralement le même pour tous ses produits, il peut être connu d'un grand nombre de personnes, ce qui compromet la sécurité du système. Pour assurer le caractère confidentiel du document, le destinataire serait obligé d'imprimer le document dès sa transmission par télécopieur.

iii) **Rapports de confirmation des mouvements du télécopieur**

Presque tous les télécopieurs impriment une confirmation de chaque opération. Ces rapports confirment si la transmission du document s'est faite correctement, et impriment le numéro du télécopieur récepteur ainsi que le nombre de pages transmises. Ce qui donne à l'émetteur une certaine assurance que les documents ont été transmis correctement. Le destinataire peut se servir du rapport pour vérifier que toutes les pages transmises ont bien été reçues.

2.4 Environnement de l'utilisateur

L'emplacement du télécopieur peut considérablement influencer le caractère sécuritaire des transmissions par télécopieur. Dans certains bureaux, les télécopieurs se trouvent dans des endroits relativement publics, donc à la portée de presque n'importe qui, ce qui donne au personnel non autorisé la possibilité de prendre connaissance des renseignements d'arrivée. Dans de telles conditions, il est plus difficile de maintenir le caractère confidentiel des renseignements personnels.

Autre problème : l'émetteur est rarement au courant des circonstances entourant le télécopieur récepteur. Il peut transmettre des renseignements confidentiels, en prenant pour acquis que les procédures du bureau récepteur offrent toute garantie de sécurité, alors que ce n'est pas le cas. C'est ainsi que l'utilisation non normalisée des télécopieurs dans les bureaux peut compromettre la confidentialité des documents.

3. DIRECTIVES

3.1 Renseignements personnels et documents faisant l'objet d'une exception

Étant donné les limitations de la technologie actuelle des télécopieurs courants, il est douteux qu'on puisse atteindre le niveau de protection de la vie privée requis par la *loi*. Il est donc recommandé de ne pas transmettre par télécopieur les renseignements personnels et les documents faisant l'objet d'une exception, selon la définition de la *loi*.

Dans les cas d'urgence où le destinataire veut qu'on utilise le télécopieur comme mode de communication, l'émetteur ne devrait transmettre les renseignements qu'à une boîte à lettres confidentielle. C'est la seule façon de transmettre des renseignements personnels, de nature particulièrement délicate. À défaut de boîte à lettres confidentielle, on ne doit jamais transmettre de renseignements personnels ni de documents faisant l'objet d'une exception par télécopieur.

Cependant, si l'on supprime toute identification individuelle d'un document à transmettre, ledit document ne peut plus être considéré comme "renseignements personnels" selon la définition de la *loi*. Avec la suppression de l'identificateur individuel, le document n'est plus "sous une forme qui permette **l'identification** individuelle", ce qui devrait en permettre la transmission par télécopieur. La suppression de renseignements personnels permettrait aussi la transmission par télécopieur de documents de cette nature.

3.2 Documents généraux

i) Le télécopieur ne devrait être utilisé que par les personnes autorisées.

Les personnes autorisées à utiliser le télécopieur sont généralement le personnel de bureau. Pour un bureau petit ou moyen, on peut charger une seule personne de transmettre les documents. Pour un bureau plus grand, ayant un gros volume de transmissions par télécopieur, il est souhaitable de centraliser les opérations. En réservant l'utilisation du télécopieur aux personnes désignées, on réduit les possibilités d'indiscrétion, en cas de transmission de renseignements confidentiels par inadvertance.

- Il faudrait charger une seule personne (et un remplaçant) du maniement du télécopieur pour qu'en cas de problème, technique ou autre, le personnel sache à qui s'adresser.

- Il faudrait installer le télécopieur dans un endroit :

  - qui ne soit pas public;

  - facile à surveiller par la personne en charge;

  - où seul le personnel autorisé ait accès aux renseignements transmis par télécopieur.

- Les institutions obligées de se servir d'un télécopieur pour communiquer des renseignements demandant une précaution particulière pourraient équiper leur télécopieur d'un verrou de sécurité.

- Les bureaux d'une institution ne devraient pas avoir de télécopieurs en commun, car cela suppose l'allocation ou le partage de boîtes à lettres confidentielles, ce qui complique encore les procédures de sécurité.

ii) Il faudrait mettre en place une marche à suivre pour garantir que les renseignements sont transmis au numéro de télécopieur voulu.

Alors qu'on peut renvoyer à l'expéditeur une enveloppe incorrectement libellée, un document envoyé au mauvais numéro peut être lu par un certain nombre de personnes. Pour éviter cette situation, les institutions devraient prendre les dispositions voulues pour que les documents soient adressés au bon numéro de télécopieur.

- Il faudrait maintenir une liste permanente de numéros de télécopieur autorisés à titre de référence.

- Le numéro de télécopieur du destinataire devrait être reconfirmé avant la transmission du document. Le numéro de télécopieur composé est affiché sur un écran semblable à celui d'un calculateur électronique. Avec les télécopieurs d'aujourd'hui, on peut confirmer le numéro du télécopieur récepteur en vérifiant personnellement le numéro affiché à l'écran avant de transmettre le document.

- Il faudrait que tous les télécopieurs des institutions gouvernementales puissent imprimer les rapports de confirmation et les rapports "historiques" des mouvements du télécopieur.

- L'émetteur devrait vérifier le rapport de confirmation des mouvements du télécopieur pour s'assurer de l'exactitude du numéro du télécopieur récepteur. Ce rapport devrait être conservé avec l'original du document télécopié. Le rapport de confirmation des mouvements du télécopieur fournit la preuve que le document a été transmis au numéro de télécopieur voulu.

- Si un document a été transmis au mauvais numéro de télécopieur, l'émetteur doit se mettre immédiatement en rapport avec l'organisme en question, l'informer de l'erreur et s'assurer que le document télécopié a été détruit.

iii) Il faut que les renseignements soient transmis au complet et en toute sécurité.

- L'expéditeur doit confirmer la bonne transmission du document en vérifiant le rapport de confirmation des mouvements du télécopieur.

- Il faut que tous les télécopieurs utilisés par les institutions gouvernementales soient équipés de boîtes à lettres confidentielles. Il faut transmettre tout document à protéger à une boîte à lettres confidentielle. Les institutions gouvernementales doivent vérifier si tel ou tel document général demande des précautions particulières à cause de la nature délicate du contenu.

iv) Le renseignement doit atteindre le destinataire concerné.

Même si on envoie le renseignement au bon numéro de télécopieur, cela ne l'empêche pas d'atteindre le mauvais destinataire.

- La première page de tout document télécopié doit être une feuille d'accompagnement, identifiant l'expéditeur et le destinataire. Cette page identifie clairement le receveur approprié.

- Le télécopieur doit être placé de sorte que seules les personnes autorisées puissent récupérer le document (voir 3.2 (1)).

- Le destinataire paraphe le rapport de confirmation des mouvements du télécopieur. Ce rapport est conservé par la personne en charge du télécopieur. (voir 3.2 (1)).

- La personne en charge du télécopieur vérifie les rapports de confirmation des mouvements du télécopieur (confirmant la réception d'un document télécopié) pour s'assurer que les documents ont été reçus par les personnes appropriées.

- Au cas où un document est transmis au mauvais numéro de télécopieur, le receveur signale l'erreur à l'émetteur, détruit le document télécopié et consigne cette action sur le rapport de confirmation des mouvements du télécopieur. Lorsqu'on adresse un document au mauvais destinataire, celui-ci redirige le document télécopié et consigne cette action sur le rapport de confirmation des mouvements du télécopieur.

v) Les renseignements doivent être reçus au complet.

- Le receveur compare le nombre de pages reçues au nombre de pages indiquées sur la feuille d'accompagnement ou sur le rapport de confirmation des mouvements du télécopieur (à défaut de feuille d'accompagnement). S'il manque des pages, il contacte l'expéditeur et lui demande de retransmettre le document.

- On pourrait envisager la possibilité d'équiper le télécopieur d'une batterie de secours en cas de panne d'électricité. Les institutions peuvent consulter le vendeur de télécopieur à ce sujet.

- Sur chaque page reçue, le télécopieur imprime :

  - la date et l'heure de réception,
  - le numéro du télécopieur émetteur,
  - le nom et l'identification de l'expéditeur, et
  - le numéro de page du document.

Sidney B. Linden
Commissaire

Ann Cavoukian, Ph.D.
Directrice de la vérification